IN THE CLAIMS

1. (Currently Amended) A method for handling on a wireless mobile communication device a secure message to be sent from the wireless mobile communication device to a recipient, comprising the steps of:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the ~~message recipient's~~ security key associated with the message recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on ~~to~~ the mobile device~~'s user~~.

2. (Currently Amended) The method of claim 1, wherein a message is provided via the user interface ~~to the user~~ indicating ~~the reason~~ that a problem exists with respect to sending ~~a~~ the secure message to the recipient in addition to indicating the reason related to the problem.

3. (Currently Amended) The method of claim 1, further comprising the step of ~~allowing the user to resolve~~ resolving the validity check issue through use of the information provided in the validity check reason, wherein the secure message is sent after resolution of the validity check issue by the user.

4. (Currently Amended) The method of claim 1, wherein the security key is a public key, wherein a user composes ~~a~~ the secure message, wherein the composed message is to be encrypted using the recipient's public key.

5. (Currently Amended) The method of claim 4, further comprising the steps of:

creating a list of all ~~of the~~ recipients for the ~~outgoing~~ composed message;

receiving data about the recipients' public keys that includes certificate information associated with the recipients; and

performing the validity check with respect to the certificate information associated with the recipients.

6. (Currently Amended) The method of claim 1, further comprising the steps of:

determining whether a certificate for a an intended recipient can be located;

providing as a validity check reason that ~~an~~ the intended ~~message~~ recipient's certificate was not located.

7. (Currently Amended) The method of claim 6 further comprising the step of removing ~~, wherein the user is allowed to remove~~ a recipient whose certificate was not located before sending a secure message to another recipient.

8. (Currently Amended) The method of claim 6 further comprising the step of ~~, wherein the user is allowed to cancel~~ canceling sending the message to a recipient whose certificate was not located.

9. (Currently Amended) The method of claim 6, further comprising the step of:

determining whether the certificate for the intended ~~a~~ recipient is locally available on the mobile device.

10. (Currently Amended) The method of claim 6, further comprising the step of:

determining whether the certificate for ~~a~~ the intended recipient is remotely available.

11. (Currently Amended) The method of claim 6~~5~~, further comprising the step of collating certificates that correspond to the recipients before performing the validity check.

12. (Currently Amended) The method of claim 6, wherein the message is to be encrypted using a Secure Multipurpose Internet Mail Extensions (S/MIME) scheme or a Pretty Good Privacy (PGP) scheme.

13. (Currently Amended) The method of claim 1, wherein the received data about ~~a recipient's~~ the security key associated with the recipient includes whether a recipient's certificate is permitted to be used;

wherein the validity check issue indicates that the recipient's certificate is not permitted to be used.

14. (Currently Amended) The method of claim 13, wherein the data about ~~permission~~ whether the ~~to use a~~ recipient's certificate is permitted to be used ~~certification~~ is based on a usage field contained in the certificate.

15. (Currently Amended) The method of claim 13, wherein the data about ~~permission~~ whether the ~~to use a~~ recipient's certificate is permitted to be used ~~certification~~ is based on a control file installed on the mobile device that specifies which ~~certifications~~ certificates are allowed to be used.

16. (Currently Amended) The method of claim 1, wherein the issue involves a validity check failure, said method further comprising the step of providing the reason of the validity check failure to the user interface on the mobile device~~'s user~~.

17. (Currently Amended) The method of claim 1, wherein the received data about ~~a recipient's~~the security key associated with the recipient includes strength of the recipient's certificate; and

wherein the validity check issue is directed to whether the recipient's certificate is permitted to be used based upon the strength of the recipient's certificate.

18. (Currently Amended) The method of claim 1, wherein the received data about ~~a recipient's~~ the security key associated with the recipient includes whether the recipient's certificate is trusted, and wherein a decision to include a recipient for a secure message is based upon whether the recipient's certificate is trusted.

19. (Currently Amended) The method of claim 1, wherein the received data about ~~a recipient's~~ the security key associated with the recipient includes validity and revocation status of a recipient's certificate, and wherein a decision to include ~~a~~ the recipient for a the secure message is based upon the validity and revocation status of ~~a~~ the recipient's certificate.

20. (Currently Amended) The method of claim 1, wherein the ~~mobile device's user decides to send~~ the message is sent to ~~a~~ the recipient despite ~~being notified~~ notification of the validity check issue.

21. (Original) The method of claim 1, wherein means for providing a wireless network and means for providing a message server are used to transmit the secure message from the mobile device.

22. (Original) The method of claim 1, wherein the mobile device is a handheld wireless mobile communications device or a personal digital assistant (PDA).

23. (Canceled)

24. (Canceled)

25. (Currently Amended) An apparatus for handling on an electronic device a secure message to be sent from the electronic device to a recipient, comprising:

a secure message processing module for use with a messaging client that sends electronic messages to recipients;

wherein the secure message processing module receives data about a security key associated with the recipient;

wherein the secure message processing module uses the received data to perform a validity check with respect to using the ~~message recipient's~~ security key associated with the recipient to send a secure message to the recipient;

wherein an issue exists based upon the validity check;

~~and a~~wherein the secure message processing module is configured to determine a reason ~~is determined~~ for the validity check issue; and

wherein the secure message processing module provides the reason ~~of~~ for the validity check issue via a user interface of ~~to~~ the electronic device's ~~user~~.

26. (Currently Amended) A wireless mobile communication device that handles a secure message to be sent from the wireless mobile communication device to a recipient, comprising:

a certificate store to store certificate data;

means for using the stored certificate data to perform a validity check with respect to using the ~~message~~ recipient's security key for sending ~~the~~ a secure message to the recipient;

wherein an issue exists due to the validity check;

means for determining a reason for the validity check issue; and

means for providing the reason ~~of~~ for the validity check issue ~~to~~via a user interface of the mobile device's ~~user~~.

27. (New) A computer-readable storage medium encoded with instructions that cause a processor to perform a method for handling on a wireless mobile communication device a secure message that is to be sent from the wireless mobile communication device to a recipient, said method comprising:

receiving data at the wireless mobile communication device about a security key associated with the recipient;

using the received data to perform a validity check with respect to using the security key associated with the message recipient to send a secure message to the recipient;

wherein an issue exists due to the validity check;

determining a reason for the validity check issue;

wherein the reason for the validity check issue is provided via a user interface on the mobile device.